AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

# UNITED STATES DISTRICT COURT

for the

Southern District of Texas



In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

information associated with Facebook user ID kurt.bryant2 that is stored at premises controlled by Facebook.

Case No. **4:19MJ0727**

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| Title 18 USC § 2252A | Certain activities relating to material constituting or containing child pornography. |

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Robert J. Guerra, Special Agent
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephonically *(specify reliable electronic means).*

Date: April 25, 2019

*Judge's signature*

City and state: Houston, Texas

Dena Hanovice Palermo, United States Magistrate Judge
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISON

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK USER ID **kurt.bryant2** THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK INC. | Case No. **4:19MJ0727** |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Robert J. Guerra, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since November 2005. I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. During my assignment with the FBI, I have participated in the execution of search warrants for documents and other evidence, including computers and electronic media, in cases involving child pornography and the sexual exploitation of children. I have investigated many cases involving child pornography and the sexual exploitation of children. I have also participated in various FBI mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which

computers are used as the means for receiving, transmitting, and storing child pornography as defined in Title 18, United States Code, Section 2256.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252A (Certain activities relating to material constituting or containing child pornography), et seq, have been committed by the individual utilizing the Facebook user ID, **kurt.bryant2.** There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

## PROBABLE CAUSE

5. Between the dates of January 23, 2019, and February 11, 2019, Special Agent (SA) Dustin Grant, FBI Salt Lake City, while acting in an undercover capacity began chatting with three different KiK profiles, user "teachme.pls", user "Deep.Inside." and user ".pleasuremachine.". All three KiK user profiles were identified as members of a known child pornography group on Kik called "Yum Yum #t.rading". SA Grant observed either by way of direct chat or as a part of the KiK group listed above, all three KiK users shared Mega links that contained child pornography.

6. On or about January 23, 2019, the KiK user "teachme.pls", shared a Mega link within the KiK group called "Yum Yum #t.rading". The Mega link contained over 60 files. Your affiant has reviewed the material contained within the Mega link and determined several of the files depict child pornography as defined by Title 18, United States Code, Section 2256. Below is a description of 1 file contained within the Mega link sent by the Kik user "teachme.pls" on or about January 23, 2019:

a) **Videos (70).3GP-** This is a video file that is 37 seconds in length depicting a minor female, who appears to be under the age of 12, being orally penetrated by an adult male's penis.

7. On or about January 30, 2019, the KiK user "Deep.Inside.", shared a total of five Mega links within the KiK group called "Yum Yum #t.rading". One Mega link contained over 4GB worth of data containing over 200 files. Your affiant has reviewed the material contained within the Mega link and determined several of the files depict child pornography as defined by Title 18, United States Code, Section 2256. Below is a description of 1 file contained within the Mega link sent by the Kik user "Deep.Inside." on or about January 30, 2019:

**a) - -(8).wmv-** This is a video file that is 59 seconds in length depicting a minor female, who appears to be under the age of 5, being orally penetrated by an adult male's penis.

8. On or about February 10, 2019, the KiK user ".pleasuremachine.", shared a Mega link within the KiK group called "Yum Yum #t.rading". The Mega link contained over 11GB worth of data containing over 200 files. Your affiant has reviewed the material contained within the Mega link and determined several of the files depict child pornography as defined by Title 18, United States Code, Section 2256. Below is a description of 1 file contained within the Mega link sent by the Kik user ".pleasuremachine." on or about February 10, 2019:

**a) 2055539.jpg-** This is an image file depicting a minor female, who appears to be under the age of 14, engaged in a pose where the minor female's genitals are exposed in a lewd and lascivious manner.

9. In consideration of the above information, FBI Salt Lake City served an administrative subpoena to KiK in pursuit of subscriber information associated with the three Kik user accounts, "teachme.pls", "Deep.Inside." and ".pleasuremachine.". A response received from KiK identified three different email accounts associated with the three KiK accounts, but all three KiK accounts utilized the same IP addresses to access the KiK application. The IP addresses identified by KiK were 98.199.241.97 and 73.6.134.25. Both IP addresses were found to be owned by Comcast Communications.

10. FBI Salt Lake City served an administrative subpoena to Comcast Communications in pursuit of subscriber information for both IP addresses 98.199.241.97 and 73.6.134.25 on the dates specified in paragraphs 21-23 utilized by the three KiK accounts. Comcast provided a response and identified the subscriber for both IP addresses to be one in the

same. The subscriber information for both IP addresses provided by Comcast Communications is as follows:

| | |
|---|---|
| Subscriber Name: | Robert Thames |
| Service Address: | 13502 Utica Street<br>Houston, Texas 77015 |
| Telephone #: | 713-689-0583 |
| Type of Service: | High Speed Internet Service |
| Start Service Date: | Unknown |
| Status: | Active |

11. On or about February 22, 2019, FBI Houston received a lead package containing the investigative details relevant to the investigation as described above. Your Affiant subsequently reviewed all of the provided case materials to include the suspected files of child pornography attributed to the Mega links that were posted by the Kik users "teachme.pls", "Deep.Inside." and ".pleasuremachine." between January 23, 2019, and February 10, 2019. Your Affiant determined that the files, described in detail above in paragraphs 21-23, depict child pornography as defined by Title 18, United States Code, Section 2256.

12. On April 12, 2019, FBI Houston executed a federal search warrant at the specific address provided by Comcast Communications. Upon the execution of said search warrant authorized by United States Magistrate Judge Peter Bray, agents identified and interviewed Kurt Randall Bryant.

13. Bryant was interviewed by SA Robert J. Guerra and SA Ryan J. Shultz. After being advised of his *Miranda Rights*, Bryant agreed to make a statement. Bryant acknowledged creating and using the three KiK account detailed in paragraphs 4-6. Bryant admitted to sending the Mega links containing child pornography within the KiK group "Yum Yum #t.rading".

14. Bryant stated he could provide information regarding a female he often chats with on Facebook. Bryant identified the female as Ashley Iverson. Bryant stated he and Iverson routinely chat on Facebook and trade child pornography material. Bryant provided the interviewing agents the login information for his Facebook account (**kurt.bryant2**) in an attempt to help the FBI locate Iverson.

15. Your affiant logged into the Facebook account **kurt.bryant2** and initiated a chat conversation with Iverson. Iverson subsequently sent child pornography material on a different chat application. In an effort to memorialize the Facebook chat conversation with Iverson, your

affiant came across several old chat conversations between Bryant and Iverson. Your affiant observed several images and at least one video that appeared to depict child pornography. One of the images observed on the Facebook account **kurt.bryant2** is described below:

a) an image file depicting an adult male displaying his erect penis with what appeared to be a minor female in the background.

16. Your affiant did not review the chat conversation between Bryant and Iverson any further. The review was stopped and a preservation letter was sent to Facebook for the Facebook account **kurt.bryant2** on April 16, 2019.

17. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

18. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

19. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

20. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A

Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

21. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

22. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

23. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

24. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

25. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

26. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

27. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

28. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

29. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

30. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

31. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts

between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

32. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning

subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

35. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

36. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Robert J. Guerra
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to telephonically on the 25th, day of April 2019.

Dena Palermo
Dena Hanovice Palermo
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

## Property to Be Searched

This warrant applies to information associated with the Facebook user ID **kurt.bryant2** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

# ATTACHMENT B

## Particular Things to be Seized

### I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including **for user ID kurt.bryant2:** full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities **from July 1, 2018 to the present.**

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them **from July 1, 2018 to the present.**, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user **from July 1, 2018 to the present.**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account **from July 1, 2018 to the present.**

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within **UP TO 14 DAYS** of service of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252A (Certain activities relating to material constituting or containing child pornography), et seq ,involving the individual utilizing the Facebook user ID, **kurt.bryant2** since **July 1, 2018**, including, for each user ID identified on Attachment A, information pertaining to the following matters:

(a) The sending/receiving of child pornography material via the Facebook chat feature. Child pornography material is currently stored on the history of the chat conversation between **kurt.bryant2** and another Facebook user.

(b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and

b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature